METHOD AND SYSTEM FOR PERMITTING USE OF IC CARD SERVICE TO MULTIPLE SERVICE USER

Patent number: JP2004102784

Publication date: 2004-04-02

Inventor: HASHIMOTO JUNKO; KASHIWAGI TAKUMI; NIWANO EIICHI; MINAMI HIROYUKI

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: ***G06F15/00; G06K17/00; G09C1/00; H04L9/32;*** **G06F15/00; G06K17/00; G09C1/00; H04L9/32;** (IPC1-7): G06F15/00; G06F17/60; G06K17/00; G09C1/00; H04L9/32

- european:

Application number: JP20020265385 20020911

Priority number(s): JP20020265385 20020911

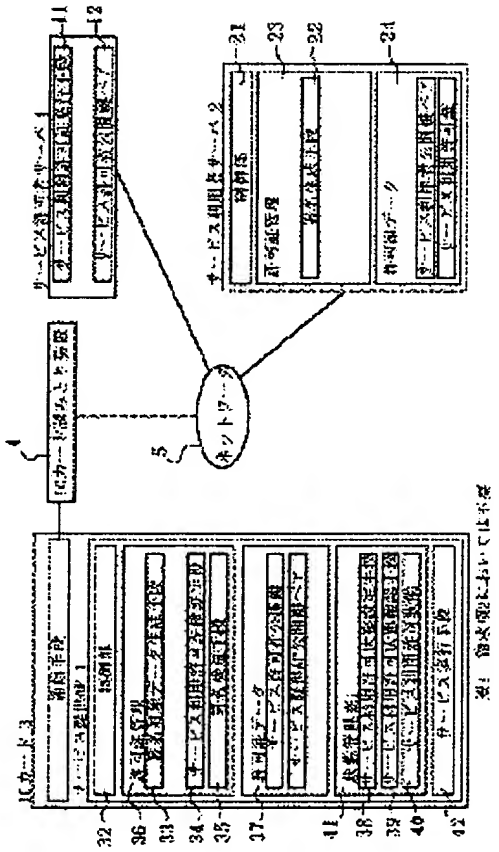
Report a data error here

Abstract of **JP2004102784**

PROBLEM TO BE SOLVED: To provide a method and a system for permitting use of IC card service allowing a service providing application in an IC card to be used by multiple enterprises.

SOLUTION: This system comprises a service permitting person's server, one or more service user servers, and IC cards used by inserting an IC card reader having a means for communicating with the service user servers. The service permitting person's server issues a use permission certificate for the service providing application stored in the IC card to one or more service user servers. The service providing application stored in the IC card verifies the service use permission certificate sent from the service user servers and, after the authentication, performs the service only when the type of the service requested by a service execution request from the service user servers matches the type of the service included in the service use certificate.

COPYRIGHT: (C)2004,JPO



Data supplied from the ***esp@cenet*** database - Worldwide

BEST AVAILABLE COPY

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-102784
(P2004-102784A)
(43)公開日　平成16年4月2日(2004.4.2)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06F	15/00	G06F	15/00	330G	5B058
G06F	17/60	G06F	17/60	126A	5B085
G06K	17/00	G06K	17/00	L	5J104
G09C	1/00	G09C	1/00	640D	
H04L	9/32	H04L	9/00	675B	

審査請求 未請求　請求項の数 12　OL　（全 19 頁）　最終頁に続く

(21)出願番号　特願2002-265385(P2002-265385)
(22)出願日　平成14年9月11日(2002.9.11)

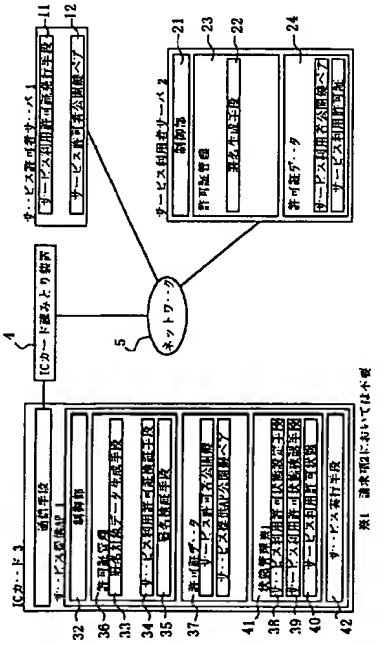
特許法第３０条第１項適用申請有り　２００２年３月１５日　社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告　信学技報　Ｖｏｌ．１０１　Ｎｏ．７４２」に発表

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100072051
弁理士　杉村　興作
(72)発明者　橋本　順子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　柏木　巧
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　庭野　栄一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】複数サービス利用者に対するＩＣカードサービス利用許可方法及びシステム

(57)【要約】
【課題】ＩＣカード内のサービス提供アプリケーションを複数の事業者に対して利用可能とするＩＣカードサービス利用許可方法及びシステムを提供することにある。
【解決手段】サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードを備えたシステムにおいて、　サービス許可者サーバが、１つ以上のサービス利用者サーバに対し、ＩＣカードに格納されたサービス提供アプリケーションの利用許可証を発行し、ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから送られてくるサービス利用許可証を検証し、認証後に、サービス利用者サーバからのサービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う。
【選択図】　図４



【特許請求の範囲】
【請求項１】
サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードからなるシステムにおいて、
サービス許可者サーバが、１つ以上のサービス利用者サーバに対し、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報（ＡＩＤ）と、サービスの種類（オペレーションの種類）を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス利用許可証を発行し、
サービス利用許可証を持つサービス利用者サーバは、ＩＣカード内に格納されたサービス提供アプリケーションを利用する際に、ＩＣカードに格納されたサービス提供アプリケーションから受け取ったチャレンジなどの署名対象データをサービス利用者秘密鍵で暗号化して署名を作成し、その署名データとサービス利用許可証をＩＣカードに格納されたサービス提供アプリケーションに送信し、
ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、
これらの検証が成功したとき、サービス利用許可証に含まれるサービス利用許可情報を記録するとともに、サービス利用許可証の検証の成功をサービス利用者サーバに返送し、
サービス利用者サーバから、サービス利用許可証に対応するサービスの実行要求を受信したとき、保持したサービス利用許可情報を確認し、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする、
ＩＣカードサービス利用許可方法。
【請求項２】
請求項１に記載の方法において、
サービス利用者サーバは、ＩＣカードに格納されたサービス提供アプリケーションから署名対象データを受け取った後に、この署名対象データとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともにＩＣカードに送り、
ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、
これらの検証が成功したとき、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする、
ＩＣカードサービス利用許可方法。
【請求項３】
請求項１又は２に記載の方法において、
サービス許可者サーバは、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス提供許可証を発行し、
サービス利用者サーバは、チャレンジなどの署名対象データをＩＣカードに送り、
ＩＣカード内のサービス提供アプリケーションは、受信した署名対象データに対しサービス提供アプリケーションの秘密鍵で署名を行い、その署名データと、サービス提供許可証をサービス利用者サーバに送り、

サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、保持しているサービス許可者公開鍵を用いてサービス提供許可証を検証するとともに、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証することを特徴とする、
ＩＣカードサービス利用許可方法。
【請求項４】
請求項１～３の何れかに記載の方法において、
サービス利用許可証のデータに、当該サービス提供アプリケーションが管理するデータの種類が含まれ、
サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみであることを特徴とする、
ＩＣカード利用許可方法。
【請求項５】
請求項１～４の何れかに記載の方法において、
サービス許可者サーバが、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する、ことを特徴とするＩＣカードサービス利用許可方法。
【請求項６】
サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードからなるシステムにおいて、
サービス許可者サーバが、１つ以上のサービス利用者サーバに対し、サービス利用許可証を発行するサービス利用許可証発行手段を持ち、
サービス利用許可証は、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報（ＡＩＤ）と、サービスの種類（オペレーションの種類）、を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、
ＩＣカードに格納されたサービス提供アプリケーションは、チャレンジなどを生成する署名対象データ生成手段を持ち、
サービス利用者サーバは、サービス利用許可証を保持しており、ＩＣカードに格納されたサービス提供アプリケーションから受け取った署名対象データにサービス利用者サーバの秘密鍵で署名を行う、署名生成手段を持ち、
ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データと、サービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証する、サービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する、署名検証手段と、
検証が成功した場合に、サービス利用許可証に含まれるサービス利用許可情報を保持するサービス利用許可状態設定手段を持ち、
サービス利用者サーバから、サービス実行要求が送信された場合に、保持したサービス利用許可情報を確認するサービス利用許可状態確認手段を持ち、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことを特徴とする、
ＩＣカードサービス利用許可システム。
【請求項７】
請求項６に記載のシステムにおいて、
ＩＣカードに格納されたサービス提供アプリケーションは、チャレンジなどを生成する署名対象データ生成手段を持ち、

サービス利用者サーバは、サービス利用許可証を保持しており、ＩＣカードに格納されたサービス提供アプリケーションへのサービス実行要求を含むデータもしくはそのダイジェスト情報に、サービス利用者サーバの秘密鍵で署名を行う、署名生成手段を持ち、
ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データと、サービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証する、サービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する、署名検証手段と、
検証が成功した場合に、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことを特徴とする、
ＩＣカードサービス利用許可システム。
【請求項８】
請求項６又は７に記載のＩＣカードサービス利用許可システムにおいて、
サービス許可者サーバが、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供許可証を発行するサービス提供許可証発行手段を持ち、
サービス提供許可証は、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、
サービス利用者サーバが、チャレンジなどを生成する署名対象データ生成手段を持ち、
サービス提供アプリケーションが、サービス利用者サーバから受け取った署名対象データに対し、サービス提供アプリケーションの秘密鍵で署名を行う、署名生成手段を持ち、
サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証する署名検証手段と、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段を持つことを特徴とする、
ＩＣカードサービス利用許可システム。
【請求項９】
請求項６～８の何れかに記載のＩＣカードサービス利用許可システムにおいて、
サービス利用許可証の署名対象データに、当該サービス提供アプリケーションが管理するデータの種類が含まれ、
サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみであることを特徴とする、
ＩＣカード利用許可システム。
【請求項１０】
請求項６～９の何れかに記載のＩＣカードサービス利用許可システムにおいて、
サービス許可者サーバが、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する、課金情報登録手段を持つことを特徴とする、
ＩＣカードサービス利用許可システム。
【請求項１１】
請求項１～５の何れかに記載の方法を実行するためのコンピュータプログラム。
【請求項１２】
請求項１１記載のコンピュータプログラムを記録したコンピュータ読取可能記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はＩＣカードサービス提供システムに関し、特に、ＩＣカード内のサービス提供ア

プリケーションを複数の事業者が利用することを可能とするＩＣカードサービス利用許可方法及びシステムに関する。

【０００２】

【従来の技術】

従来のＩＣカードサービスシステムでは、サービス提供アプリケーションへのアクセス制御を行う主体と、サービス提供アプリケーションへの（アクセス制御の対象となる）アクセスを行う主体は、分離されていなかった。

そして、サービス提供アプリケーションが、適切なサービス利用者サーバに対してのみサービス提供を行うために、アクセス制御を行う場合、そのアクセス制御の基となる情報を、実際にアクセス制御の対象となるアクセスが行われる前に、サービス提供アプリケーションに予め設定していた。

以降、このアクセス制御の基となる情報を、暗号コードと呼ぶ。この暗号コードは、共通鍵・公開鍵である場合もある。この暗号コードと、暗号コードに対応するアクセス時の入力情報を、サービス提供アプリケーションに含まれる認証プロトコルに入力することによって、サービス提供アプリケーションは、正当なアクセス者を認証することができる。

従って、アクセス者は、暗号コードに対応する入力情報を作成する手段及び情報を保持しておく必要がある。この手段及び情報は、最も単純な場合には、サービス提供アプリケーションの持つ暗号コードと一致する暗号コードであり、認証プロトコルとして共通鍵認証を用いる場合には、サービス提供アプリケーションが持つ暗号コードである共通鍵で任意の情報を暗号化したものである。

従来のＩＣカードサービスシステムでは、ＩＣカード内のサービス提供アプリケーションに暗号コードを設定した主体が、同時に暗号コードに対応する入力情報を作成する手段及び情報を保持しており、サービス提供アプリケーションへのアクセスを行っていた。

【０００３】

【発明が解決しようとする課題】

しかし、これら暗号コードに対応する入力情報を作成する手段及び情報を、他の事業主体に安全に分配する手段については、発明されていなかった。

従って、従来のＩＣカードシステムでは、以下のような問題があった。

第一の問題点は、１つのサービス提供アプリケーションを複数の事業者で安全に共有することができないことである。

第二の問題点は、１つのサービス提供アプリケーションが保持する情報を複数の事業者で共有することができないことである。

第三の問題点は、１つのサービス提供アプリケーションを複数の事業者に共有した場合に、適切な課金の仕組みがないことである。ここで、サービス提供アプリケーションは、同一カード内の他のサービス提供アプリケーションによって利用されるライブラリのようなサービス提供アプリケーションも含むとする。

このため、あるサービス利用者がサービス提供アプリケーションの機能を利用する場合には、同一機能を持ったサービス提供アプリケーションが既にＩＣカード内に存在していても、自分専用のサービス提供アプリケーションを新たにＩＣカードに格納する必要があった。

従って、従来、利用者は、あるサービスの提供を複数の事業者から受ける場合に、その機能を持ったサービス提供アプリケーションを、複数、カード内に持つ必要があった。

【０００４】

本発明の目的は、これらの問題点を解決し、あるサービス提供アプリケーションを保持する業者が、他事業者に対し、安全にそのサービス利用権を貸与できる方法及びシステムを提供することにある。また、その際、貸与に対する課金の仕組みを提供することにある。これらの仕組みによって、複数の事業者がサービス提供アプリケーションを開発することなく、容易にサービスの提供を受けることが可能となる。また、１つのサービス提供アプリケーションを複数の事業者が共有することによって生まれる、付加価値サービスが可能となる。

【０００５】
【課題を解決するための手段】
これらの問題を解決するために、請求項１に記載の発明は、
サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードからなるシステムにおいて、
サービス許可者サーバが、１つ以上のサービス利用者サーバに対し、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報（ＡＩＤ）と、サービスの種類（オペレーションの種類）を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス利用許可証を発行し、
サービス利用許可証を持つサービス利用者サーバは、ＩＣカードに格納されたサービス提供アプリケーションを利用する際に、ＩＣカードに格納されたサービス提供アプリケーションから受け取った署名対象データをサービス利用者公開鍵で暗号化して署名を作成し、その署名データとサービス利用許可証をＩＣカードに格納されたサービス提供アプリケーションに送信し、
ＩＣカードに格納されたサービス提供アプリケーションは、受信した署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、
これらの検証が成功したとき、サービス利用許可証に含まれるサービス利用許可情報を記録するとともに、サービス利用許可証の検証の成功をサービス利用者サーバに返送し、
サービス利用者サーバから、サービス利用許可証に対応するサービスの実行要求を受信したとき、保持したサービス利用許可情報を確認し、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする。
【０００６】
また、請求項６記載の発明は、この請求項１記載の方法を実施するシステムであって、サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードからなるシステムにおいて、
サービス許可者サーバは、１つ以上のサービス利用者サーバに対し、サービス利用許可証を発行するサービス利用許可証発行手段を持ち、
サービス利用許可証は、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報（ＡＩＤ）と、サービスの種類（オペレーションの種類）、を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、
ＩＣカードに格納されたサービス提供アプリケーションは、チャレンジなどの署名対象データを生成する署名対象データ生成手段を持ち、
サービス利用者サーバは、サービス利用許可証を保持しており、ＩＣカードに格納されたサービス提供アプリケーションから受け取った署名対象データにサービス利用者サーバの秘密鍵で署名を行う署名生成手段を持ち、
ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する署名検証手段と、
検証が成功した場合に、サービス利用許可証に含まれるサービス利用許可情報を保持するサービス利用許可状態設定手段を持ち、
サービス利用者サーバから、サービス実行要求が送信された場合に、サービス利用許可情報を確認するサービス利用許可状態確認手段を持ち、サービス実行要求で要求されたサー

ビスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことをとする。

【０００７】

請求項１及び６に記載の発明では、サービス利用許可証を持つ者のみが、サービス提供アプリケーションによって、サービス利用許可証で指定されたサービスの提供を受けることができる。また、サービス利用許可証は、複数の業者に対して、サービスの種類を指定して発行が可能である。

従って、サービス許可者は、サービス提供アプリケーションを利用してよいサービス利用者サーバと事前に契約を行ってサービス利用許可証を発行することで、複数のサービス利用者に対して、きめ細やかなサービスの利用許可を行うことができる。

さらに、サービス利用許可証を発行するためには、サービス許可者の秘密鍵で署名を行うことが必要であるため、サービス利用許可証の第三者による不正な発行を防ぐことが可能である。また、サービス利用許可証にはサービス利用者の公開鍵が含まれるため、サービス利用許可証の第三者による不正な利用を防ぐことが可能である。

従って、本発明は、上記技術により、あるサービス提供アプリケーションを実行する権限を持つサービス許可者が、そのサービス提供アプリケーションを実行する権限を、複数のサービス利用者に対して安全に委譲することを可能としている。

【０００８】

請求項２に記載の発明は、請求項１に記載の方法において、

サービス利用者サーバは、ＩＣカードに格納されたサービス提供アプリケーションから署名対象データを受け取った後に、この署名対象データとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともにＩＣカードに送り、

サービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、

これらの検証が成功したとき、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする。

【０００９】

また、請求項７記載の発明は、請求項２に記載の方法を実施するシステムであって、請求項６記載のシステムにおいて、

サービス利用者サーバは、ＩＣカードに格納されたサービス提供アプリケーションから受け取った署名対象データとサービス提供アプリケーションへのサービス実行要求を含むデータもしくはそのダイジェスト情報に、サービス利用者サーバの秘密鍵で署名を行う署名生成手段を持ち、

ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する署名検証手段と、

検証が成功した場合に、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うサービス実行手段を持つことを特徴とする。

【００１０】

請求項１及び６に記載の発明では、サービス提供アプリケーションからサービスの提供を受けるにあたって、事前にサービス利用許可証を提示し、認証を行っていたが、請求項２及び７に記載の発明では、事前の認証は行わず、サービス提供アプリケーションへのサービス要求時に、サービス利用許可証の確認を行うものである。

【００１１】

請求項３記載の発明は、請求項１又は２記載の方法において、
サービス許可者サーバは、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス提供許可証を発行し、
サービス利用者サーバは、チャレンジなどの署名対象データをＩＣカードに送り、
ＩＣカード内のサービス提供アプリケーションは、受信した署名対象データに対しサービス提供アプリケーションの秘密鍵で署名を行い、その署名データと、サービス提供許可証をサービス利用者サーバに送り、
サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、保持しているサービス許可者公開鍵を用いてサービス提供許可証を検証するとともに、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証する、
ことを特徴とする。
【００１２】
また、請求項８に記載の発明は、請求項３に記載の方法を実施するシステムであって、請求項６又は７記載のシステムにおいて、
サービス許可者サーバは、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供許可証を発行するサービス提供許可証発行手段を持ち、
サービス提供許可証は、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションの識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、
サービス利用者サーバは、チャレンジなどの署名対象データを生成する署名対象データ生成手段を持ち、
サービス提供アプリケーションは、サービス利用者サーバから受け取った署名対象データに対し、サービス提供アプリケーションの秘密鍵で署名を行う、署名生成手段を持ち、
サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証する署名検証手段と、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段を持つことを特徴とする。
【００１３】
請求項１～２及び６～７に記載の発明では、サービス提供アプリケーションが、適切なサービス利用者を確認するための手段を提供していたが、請求項３及び８に記載の発明では、サービス利用者サーバが、通信相手である、サービス提供アプリケーションを確認する手段を提供している。
従って、請求項３及び８に記載の発明は、あるサービス提供アプリケーションを実行する権限を持つサービス許可者から、そのサービス提供アプリケーションを実行する権限を委譲された複数のサービス利用者が、不正なサービス提供アプリケーションからサービスの提供を受けることなく、安全にサービス利用することを可能としている。
従って、本発明によれば、あるサービス提供アプリケーションが提供するサービスを複数のサービス提供者間で安全に共有することが可能となる。
【００１４】
請求項４又は９に記載の発明は、請求項１～３又は６～８の何れかに記載の方法又はシステムにおいて、
サービス利用許可証の署名対象データに、当該サービス提供アプリケーションが管理するデータの種類が含まれ、
サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみ

である、
ことを特徴とする。
【００１５】
請求項１～３又は６～８に記載の発明では、サービス利用許可の対象が、サービス提供アプリケーションの提供するサービスの種類（オペレーションの種類）であったが、請求項４、９に記載の本発明にあっては、サービス利用許可の対象として、そのサービス（オペレーション）が対象とするデータの種類まで限定することによって、細やかなサービス利用許可を実現するものである。
従って、本発明によれば、あるサービス提供アプリケーションが保持するデータを複数のサービス利用許可者間で安全に共有することが可能となる。
【００１６】
請求項５又は１０に記載の本発明は、請求項１～４又は６～９の何れかに記載の方法又はシステムにおいて、
サービス許可者サーバは、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する課金情報登録手段を持つことを特徴とする。
請求項５及び１０に記載の発明では、請求項１～４又は６～９に記載の方法及びシステムで発行されたサービス利用許可証を、課金情報として利用する手段を提供している。
【００１７】
【発明の実施の形態】
次に、本発明の実施の形態について図面を参照して詳細に説明する。
図１は、請求項１～５に記載の本発明によるＩＣカードサービス利用許可方法を実施する請求項６～１０に記載のシステムの全体構成を示す。１はサービス提供者サーバ、2_1，2_2，．．．2_nは複数のサービス利用者サーバ１，２，．．．ｎ、3_1，3_2，．．．3_nはＩＣカード、４はＩＣカード読取装置４、５はＩＣカード読取装置４とサービス提供者サーバ１とサービス利用者サーバ１，２，．．．ｎを相互接続するネットワーク５である。
【００１８】
サービス許可者サーバ１は、複数のサービス提供アプリケーションＡＰ１，ＡＰ２，．．．ＡＰｎを複数のＩＣカード１，２，．．．ｎに提供しており、サービス提供アプリケーションを利用する複数のサービス利用者サーバ１，２，．．．ｎへそれぞれサービス利用許可証の発行を行う。また、サービス提供アプリケーションにそれぞれ格納するサービス提供許可証を発行する。サービス利用者サーバ１，２，．．．ｎは、任意のＩＣカード内の任意のサービス提供アプリケーションと読取装置４及びネットワーク５を介して通信を行ってＩＣカード保持者にサービスを提供する。以後、サービス提供アプリケーションはサービス提供ＡＰと略記する。
ＩＣカードに格納されたサービス提供ＡＰは、サービス提供時にサービス利用許可証のチェックを行い、適切な利用者に適切な種類のサービス提供を行う。
ＩＣカード保持者は、ＩＣカード読取装置などを操作し、サービス利用者サーバ及びＩＣカードからサービスを提供される。
【００１９】
図２は、請求項３及び請求項８に記載の発明におけるＩＣカード内のサービス提供ＡＰとサービス提供許可証の関係を示す。
ＩＣカードには１つ以上のサービス提供ＡＰが格納されており、図では３つのサービス提供アプリケーションＡＰ１，ＡＰ２，ＡＰ３が格納され、そのそれぞれのサービス提供ＡＰ１，ＡＰ２，ＡＰ３は、制御部の制御の下で通信手段を介してサービス許可者から受け取ったサービス提供許可証１，２，３を保持している。
【００２０】
図３は、請求項１～４及び６～９に記載の方法及びシステムで使用するサービス利用許可証及びサービス提供許可証の構造を示す。

（α）は、請求項１～４及び６～９に記載の方法及びシステムにおいて、サービス提供者サーバがサービス利用者サーバに対し発行するサービス利用許可証を示し、このサービス利用許可証は、利用許可するサービス利用者サーバの公開鍵と、利用許可するサービス提供ＡＰのＡＩＤと、サービスの種類（オペレーションの種類）等を含むサービス利用許可情報と、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。
（ｂ）は、請求項４及び９に記載の方法及びシステムにおいて、サービス提供者サーバがサービス利用者サーバに対し発行するサービス利用許可証を示し、このサービス利用許可証は、利用許可するサービス利用者サーバの公開鍵と、利用許可するサービス提供ＡＰのＡＩＤと、サービスの種類（オペレーションの種類）と、利用許可するデータの種類等を含むサービス利用許可情報と、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。
（ｃ）は、請求項３及び８に記載の方法及びシステムにおいて、サービス提供者サーバがＩＣカードに格納されたサービス提供ＡＰに対し発行するサービス提供許可証を示し、このサービス提供許可証は、サービス提供ＡＰの公開鍵と、サービス提供ＡＰのＡＩＤ等を含むデータと、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。
【００２１】
図４は、請求項１、２に記載の本発明方法を実施するシステムの原理構成図を示す。
本システムは、ネットワーク５に接続されたサービス許可者サーバ１、サービス利用者サーバ２、ＩＣカード３、ＩＣカード読取装置４からなる。
サービス許可者サーバ１は、サービス利用許可証発行手段１１を持ち、サービス許可者公開鍵ペアを保持する保持部１２を持つ。
サービス利用者サーバ２は、制御部２１と、署名生成手段２２を持つ許可証管理部２３と、サービス利用者公開鍵ペアとサービス利用許可証などを保持する許可証データ保持部２４を持つ。
ＩＣカード３は、通信手段３１と、サービス提供アプリケーションＡＰＩを持つ。
サービス提供ＡＰＩは、制御部３２と、署名対象データ生成手段３３とサービス利用許可証検証手段３４と署名検証手段３５を持つ許可証管理部３６と、サービス許可者公開鍵とサービス提供ＡＰ公開鍵ペアなどを保持する許可証データ保持部３７と、サービス利用許可状態設定手段３８と、サービス利用許可確認手段３９と、サービス利用許可状態保持部４０を持つ状態管理部４１を持ち、更に、サービス実行手段４２を持つ。
【００２２】
図５は、これらの手段を備える図４のシステムで実行される請求項１に記載のサービス利用許可方法の手順の一例を示すフローチャートである。
本システムでは、サービス許可者サーバ１のサービス利用許可証発行手段１１が、保持部１２のサービス許可者公開鍵ペアを用いて、図３αに示すサービス利用許可証１を予め発行している。
▲１▼このようなサービス利用許可証を持つサービス利用者サーバ２は、サービス提供ＡＰの利用時に、制御部２１にて、ＩＣカード読取装置５を通し、ＩＣカード３に、チャレンジ（乱数）生成の要求を出す。
ＩＣカード３では、通信手段３１が、サービス提供ＡＰＩの制御部３２とサービス利用者サーバ２からの／への通信を仲介する。
▲２▼サービス提供ＡＰＩの制御部３２は、許可証管理部３６内の署名対象データ生成手段３３によって、乱数（チャレンジ）を生成・保存するとともに、サービス利用者サーバ２に送信する。
▲３▼サービス利用者サーバ２は、許可証管理部２３内の署名生成手段２２にて保持部２４のサービス利用者秘密鍵で、乱数を暗号化して署名を作成し、その署名データと一緒にサービス利用許可証をＩＣカード３に送信する。
▲４▼ＩＣカード３内のサービス提供ＡＰＩの制御部３２は、許可証管理部３６内の署名

検証手段３５で、受信したサービス利用許可証に含まれるサービス利用者公開鍵を用いて、受信した署名データの検証を行う。また、▲５▼サービス利用許可証検証手段３４で、許可証データ保持部３７に保持しているサービス許可者公開鍵を用いて、受信したサービス利用許可証の検証を行う。

▲６▼これらの検証が成功したときは、状態管理部４１内のサービス利用許可状態設定手段３８で、サービス利用許可証の検証が成功したことと、サービス利用許可証に含まれる許可されたサービスの種類やサービス利用者公開鍵などのサービス利用許可情報をサービス利用許可状態保持部４０に記録し、サービス利用者サーバ２に検証成功を返却する。

▲７▼サービス利用者サーバ２は、制御部２１にて、サービス利用許可証に対応するサービスの実行を要求する。

▲８▼サービス提供ＡＰｉの制御部３２は、状態管理部４１内のサービス利用許可状態確認手段３９にてサービス利用許可状態保持部４０を検索し、要求されたサービスがサービス利用許可証で許可済かどうかを確認し、許可済の場合は、▲９▼サービス実行手段４２にサービスの実行を要求する。

従って、本システムによれば、サービス提供ＡＰは事前にサービス利用許可証の提示を受け、認証を行うことにより、正当なサービス利用者サーバのみにサービス提供ＡＰの利用を許可することができる。

尚、上記の例では、サービス利用者の署名データを先に検証し、次にサービス利用許可証を検証しているが、サービス利用許可証を先に検証し、サービス利用者の署名データをあとで検証してもよく、順番は問わない。また、署名対象データとして乱数を用いているが、他のデータを用いることができる。

【００２３】

図６は請求項２に記載の方法の手順の一例を示すフローチャートである。

請求項２に記載のシステムでは、サービス提供ＡＰの利用時に、事前にサービス利用許可証の認証を行わないで、サービス提供ＡＰへのサービス実行要求時に、サービス要求許可証の認証を実行する。従って、本システムでは、▲１▼サービス利用者サーバ２は、サービス提供ＡＰ１からチャレンジを受け取った後に、制御部２１にてサービス実行要求を発生し、▲２▼署名生成手段２２にて該チャレンジとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともにＩＣカード３に送る。

▲３▼ＩＣカード３内のサービス提供ＡＰ１は、許可証管理部２３にて、受信した署名データを受信したサービス利用許可証に含まれるサービス利用者公開鍵で検証するとともに、▲４▼受信したサービス利用許可証を、保持しているサービス許可者公開鍵で検証する。

▲５▼これらの検証が成功したとき、サービス提供ＡＰは、状態管理部４１にて、サービス実行要求で要求されたサービスがサービス利用許可証に含まれるサービスの種類と一致するか確認し、▲６▼一致する場合に、サービス実行手段４２にサービスの実行を要求する。

尚、本例では、サービス実行要求と一緒にサービス提供ＡＰからのチャレンジの署名を行っているが、このチャレンジの署名は省略してもよい。

【００２４】

図７は、請求項３に記載の方法を実施する請求項８記載のシステムの原理構成図を示す。

請求項３に記載の方法は、サービス利用者サーバ２が通信相手であるサービス提供ＡＰを認証することができ、この目的のために、本システムは、図４に示す請求項６～７に記載のシステムの手段に加えて、サービス許可者サーバ１が、ＩＣカードに格納されたサービス提供ＡＰ１に、図３ｂに示すサービス提供許可証を発行するサービス提供許可証発行手段１３を備え、ＩＣカード３内のサービス提供ＡＰ１がサービス許可者サーバ１により発行されたサービス提供許可証を許可証データ保持部３７に保持するとともに、署名生成手段３８を備え、サービス利用者サーバ２がサービス許可者公開鍵を許可証データ保持部２４に保持するとともに、署名対象データ生成手段２５と、サービス提供許可証検証手段２

６と、署名検証手段２７を備える。
【００２５】
図８は請求項３に記載の方法におけるサービス提供許可証の認証手順を示す。
▲１▼サービス利用者サーバ２の制御部２１が許可証管理部２３内の署名対象データ生成手段２５によってチャレンジ（乱数）を生成してＩＣカード３に送る。
▲２▼ＩＣカード３内のサービス提供ＡＰは、許可証管理部３６内の署名生成手段３８にて、受信した乱数をサービス提供ＡＰの秘密鍵で暗号化して署名を生成し、この署名データを許可証データ保持部３７に保持しているサービス提供許可証とともにサービス利用者サーバ２に送る。
▲３▼サービス利用者サーバ２は、許可証管理部２３内の署名検証手段２７にて、受信したサービス提供許可証に含まれるサービス提供ＡＰ公開鍵を用いて、受信した署名データを検証するとともに、▲４▼サービス提供許可証検証手段２６にて、保持しているサービス許可者公開鍵を用いて、受信したサービス提供許可証を検証することにより、サービス提供ＡＰの正当性を確認する。
尚、サービス提供ＡＰの署名データの検証とサービス提供許可証の検証の順番は問わない。また、署名対象データとして乱数を用いているが、他のデータを用いることもできる。
【００２６】
【実施例】
実施例として、本発明を医療分野に適用した場合を示す。
サービス許可サーバは、医師会Ｘであり、ＩＣカードアプリケーションである、電子カルテＡＰ及び処方箋ＡＰを保持している。
サービス提供ＡＰは、これら電子カルテＡＰ及び処方箋ＡＰである。
サービス利用者サーバは、医師会Ｘからこれらサービス提供ＡＰを利用する認可を受けている病院Ａと病院Ｂ、薬局Ｃである。
病院Ａは、処方箋ＡＰに関して、処方箋書き込みサービスに関するサービス利用許可証Ａ１を保持している。
病院Ｂは、処方箋ＡＰを使用しない。
薬局Ｃは、処方箋ＡＰに関して、処方箋読み出しサービスに関するサービス利用許可証Ｃ１を保持している。
病院Ａは、電子カルテＡＰに関して、電子カルテ書き込みサービス及び電子カルテ読み出しサービスを、対象データが病院Ａの書き込みデータであるレコードに限定して許可している、サービス利用許可証Ａ２を保持している。
病院Ｂは、電子カルテＡＰに関して、電子カルテ書き込みサービス及び電子カルテ読み出しサービスを、全てのデータを対象として許可している、サービス利用許可証Ｂ２を保持している。
薬局Ｃは、電子カルテＡＰに関して、電子カルテ読み出しサービスを、対象データが全ての病院の書き込みデータである場合において、全てのデータの、病院ＩＤ、診察日、診察医名の項目のみ許可している、サービス利用許可証Ｃ２を保持している。
これらのサービス利用許可証Ａ１，Ｃ１，Ａ２，Ｂ２は、全て、サービス許可サーバである医師会Ｘより発行されている。これらのサービス利用許可証Ａ１，Ｃ１，Ａ２，Ｂ２の例を図９の（ａ）－（ｅ）に示す。
【００２７】
また、処方箋ＡＰと電子カルテＡＰを格納したＩＣカードを保有する利用者Ｄは、病院Ａ、病院Ｂ、薬局Ｃをそれぞれ利用している。
利用者ＤのＩＣカードに格納された処方箋ＡＰは、サービス提供許可証Ｄ１を保持しており、電子カルテＡＰは、サービス提供許可証Ｄ２を保持している。これらのサービス提供許可証Ｄ１及びＤ２の例を図９の（ｆ）及び（ｇ）に示す。
病院Ａ、病院Ｂ、薬局Ｃにはそれぞれ、病院Ａサーバ、病院Ｂサーバ、薬局Ｃサーバと通信を行うＩＣカード読取装置が設置されている。
【００２８】

利用者Ｄは病院Ａで処方箋の書込みサービスを受けることができる。図１０はこの場合のシーケンスの一例を示す。利用者Ｄが、病院Ａにて病院ＡのＩＣカード読取装置にＩＣカードを挿入すると、病院サーバＡは、ＩＣカード内の処方箋ＡＰと通信を行う。本例では、請求項３に記載の方法を用い、最初に、処方箋ＡＰは、病院Ａのサービス利用許可証Ａ１を確認し、病院Ａサーバは、処方箋ＡＰのサービス提供許可証Ｄ１を確認する。この目的ために、本例では、最初に、

▲１▼病院Ａサーバと処方箋ＡＰとの間でチャレンジ１及びチャレンジ２を交換する。

▲２▼病院Ａサーバは処方箋ＡＰから受け取ったチャレンジ２を病院Ａの秘密鍵で暗号化して署名を生成し、この署名データ２をサービス利用許可証Ａ１とともに処方箋ＡＰに送り、処方箋ＡＰは送られてきた署名データ２を病院Ａの公開鍵で検証するとともにサービス利用許可証Ａ１を医師会サーバの公開鍵で検証して、病院Ａのサービス利用許可証Ａ１の正当性を確認する。

▲３▼正当性の確認後、処方箋ＡＰはサービス利用許可証Ａ１に含まれるサービス利用許可情報を格納する。

▲４▼サービス利用許可情報の格納後、処方箋ＡＰは、病院Ａサーバから受け取ったチャレンジ１を処方箋ＡＰの秘密鍵で暗号化して署名を生成し、この署名データ１をサービス提供許可証Ｄ１とともに病院Ａサーバに送り、病院Ａサーバは、送られてきた署名データ１をサービス提供許可証Ｄ１に含まれる処方箋ＡＰの公開鍵で検証するとともにサービス提供許可証Ｄ１を医師会サーバの公開鍵で検証して、処方箋ＡＰのサービス提供許可証Ｄ１の正当性を確認する。

その後、病院サーバＡは、処方箋ＡＰに、処方箋情報の書き込みを行う。

【００２９】

また、利用者Ｄは病院Ａで電子カルテの書き込みサービスを受けることができる。図１１はこの場合のシーケンスの一例を示す。利用者Ｄが、病院Ａにて病院ＡのＩＣカード読取装置にＩＣカードを挿入すると、病院サーバＡは、ＩＣカード内の電子カルテＡＰと通信を行う。本例では、請求項２に記載の方法を用い、電子カルテＡＰは、病院Ａのサービス利用許可証Ａ２を確認した後に、電子カルテ情報の書き込みを行う。本例では、最初に、

▲１▼病院Ａサーバは、チャレンジ要求を電子カルテＡＰに送り、電子カルテＡＰから送られてくるチャレンジ２を受け取り、受け取ったチャレンジ２とサービス実行要求を病院Ａの秘密鍵で暗号化して署名を生成し、この署名データをサービス利用許可証Ａ２とともに電子カルテＡＰに送る。

▲２▼電子カルテＡＰは、受け取った署名データを病院Ａの公開鍵で検証するとともに、サービス利用許可証Ａ２を医師会サーバの公開鍵で検証して、病院Ａのサービス利用許可証Ａ２の正当性を確認する。

▲３▼サービス利用許可証Ａ２の確認後、電子カルテＡＰは、サービス実行要求で要求されたサービスの種類（電子カルテの書き込み）がサービス利用許可証に含まれるサービスの種類と一致するか確認し、一致する場合に、サービス実行要求を電子カルテ実行手段及び病院Ａサーバの制御部に送り、電子カルテの書き込みを行う。

【００３０】

医師会Ａは、請求項５に記載のように、サービス利用許可証の発行履歴をサーバ内に保存しており、発行履歴を参照して、病院Ａ、病院Ｂ、薬局Ｃに課金を行う。

図１２は、本実施例において、利用者Ｄが、病院Ａ、病院Ｂ、薬局Ｃでそれぞれ電子カルテに記録されたデータの読み出しサービスを受ける場合の、読み出し可能なデータ範囲を示す。

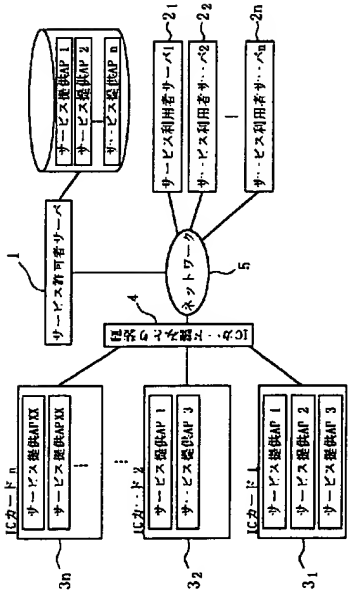
【００３１】

以上、本発明によるＩＣカードサービス利用許可方法及びシステムの構成を説明したが、本発明システムを構成するサービス提供者サーバ、サービス利用者サーバ及びＩＣカードの種々の手段はコンピュータにより実現され、本発明方法の処理手順はこえらのコンピュータにより実行され、本発明はこれらの処理手順を実行させるためのコンピュータプログラム及び該コンピュータプログラムを記録した記録媒体も本発明の範囲に含むものである

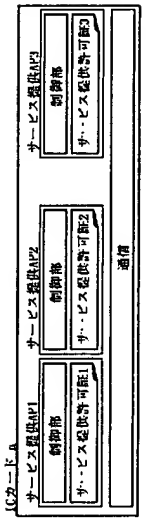
【００３２】
【発明の効果】
以上に述べたように本発明によれば、次のような効果が得られる。
（１）サービス許可者が複数のサービス利用者に対してサービス利用許可証を発行し、ＩＣカード内のサービス提供ＡＰがサービス利用許可証に基づいた実行制御を行うことによって、複数のサービス利用者が、自らはサービス提供ＡＰを開発することなく、１つのサービス提供ＡＰから提供されるサービスを利用することが可能となる。
（２）サービス利用者は、サービス提供ＡＰが持つサービス提供許可証を確認することによって、サービス提供ＡＰが、自らの保持するサービス利用許可証に対応する、正当なＡＰであることを確認することができる。
（３）サービス許可者は、複数のサービス利用者に、適切なサービスの提供を行い、サービス利用許可証を発行した代償として、サービス利用者に課金を行うことができる。
（４）複数のサービス利用者が、１つのサービス提供ＡＰを使用するため、サービス提供ＡＰに対し、あるサービス利用者が登録したデータを、他のサービス利用者が参照するなど、複数サービス利用者間での、サービス提供ＡＰのサービスの共有が可能である。
（５）同様に、複数サービス利用者間での、サービス提供ＡＰのデータの共有が可能である。
【図面の簡単な説明】
【図１】請求項１～５に記載の本発明のＩＣカードサービス利用許可方法を実施するシステムの全体構成図である。
【図２】請求項３に記載の発明におけるＩＣカード内のサービス提供ＡＰとサービス提供許可証の関係を示す図である。
【図３】請求項１～４に記載の方法で使用するサービス利用許可証及びサービス提供許可証の構造を示す図である。
【図４】請求項１、２に記載の方法を実施するシステムの原理構成図を示す。
【図５】請求項１に記載の方法の手順の一例を示すフローチャートである。
【図６】請求項２に記載の方法の手順の一例を示すフローチャートである。
【図７】請求項３に記載の方法を実施するシステムの原理構成図を示す。
【図８】請求項３に記載の方法の手順の一例を示すフローチャートである。
【図９】本発明の実施例における、サービス利用許可証Ａ１，Ｃ１，Ａ２，Ｂ２の例を示す図である。
【図１０】本発明の実施例において、利用者Ｄが、病院Ａで処方箋ＡＰの書き込みサービスを受けるサービス利用例のシーケンスを示す図である。
【図１１】本発明の実施例において、利用者Ｄが、病院Ａで電子カルテＡＰの書き込みサービスを受けるサービス利用例のシーケンスを示す図である。
【図１２】本発明の実施例において、利用者Ｄが、病院Ａ、病院Ｂ、薬局Ｃでそれぞれ電子カルテの読み出しサービスを受ける場合の、読み出し可能なデータ範囲を示す図である。
【符号の説明】
１　サービス許可者サーバ
２　サービス利用者サーバ
３　ＩＣカード
４　ＩＣカード読取装置
５　ネットワーク
ＡＰ１，．．．ＡＰｎ　サービス提供アプリケーション
１１　サービス利用許可証発行手段
１２　サービス許可者公開鍵ペア
２１　制御部
２２　署名生成手段

２３　許可証管理部
２４　許可証データ保持部
２５　署名対象データ生成手段
２６　サービス提供許可証検証手段
２７　署名検証手段
３１　通信手段
３２　制御部
３３　署名対象データ生成手段
３４　サービス利用許可証検証手段
３５　署名検証手段
３６　許可証管理部
３７　許可証データ保持部
３８　サービス利用許可状態設定手段
３９　サービス利用許可状態確認手段
４０　サービス利用許可状態保持部
４２　サービス実行手段

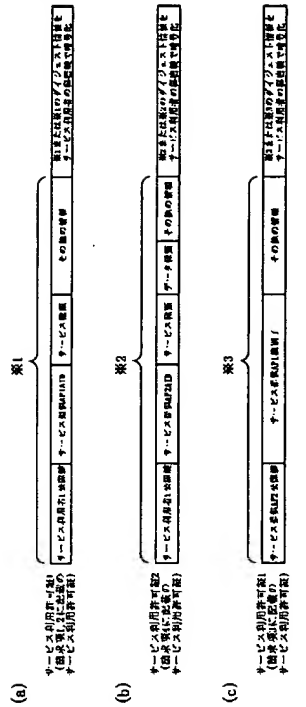
【図１】



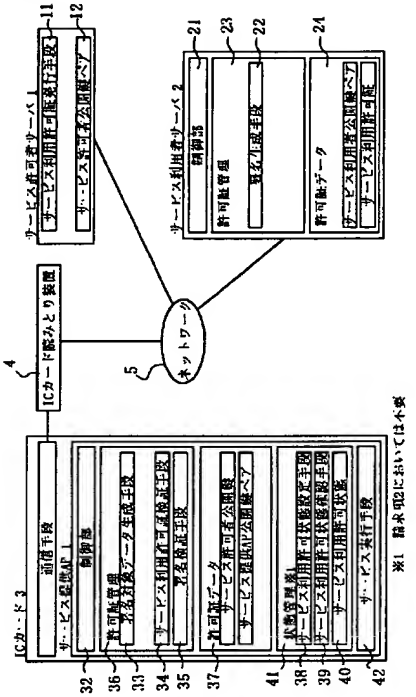
【図２】



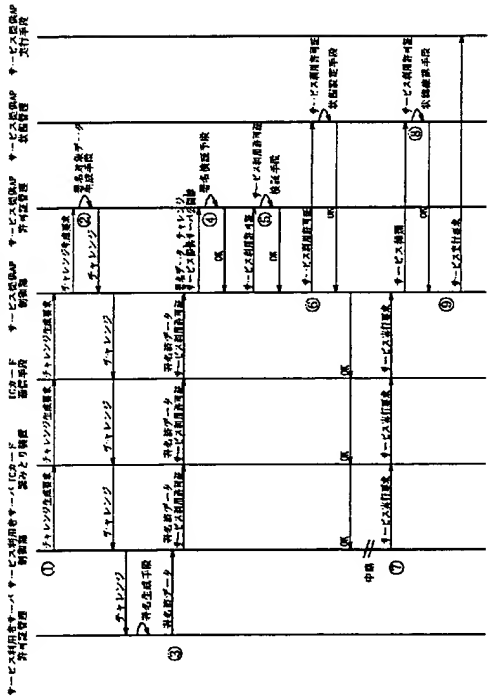
【図３】



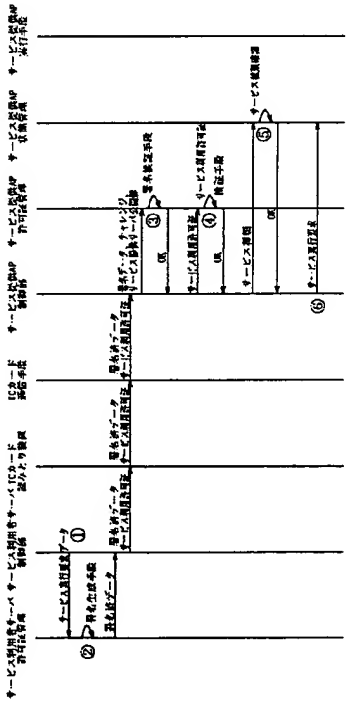
【図４】



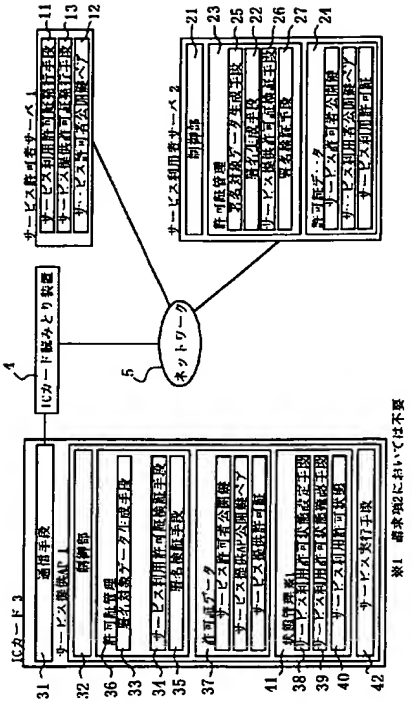
【図５】



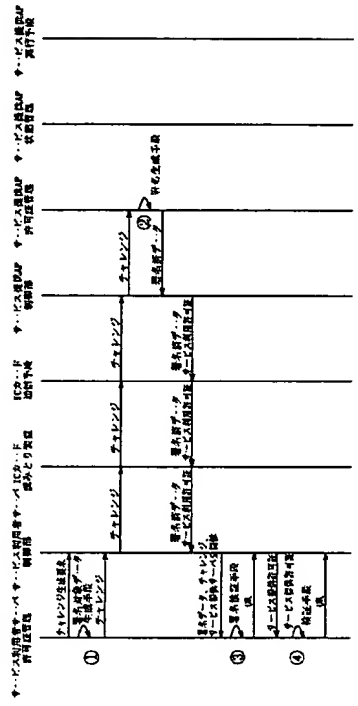
【図６】



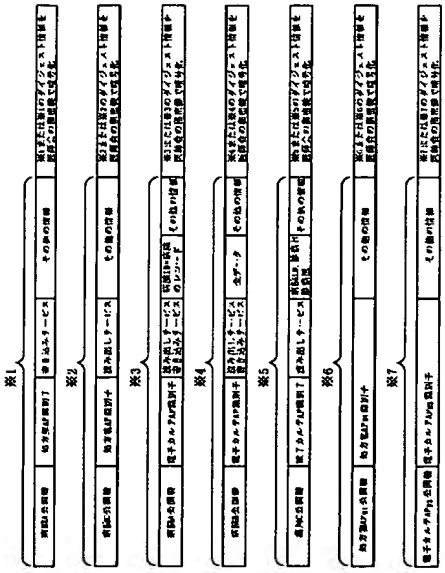
【図７】



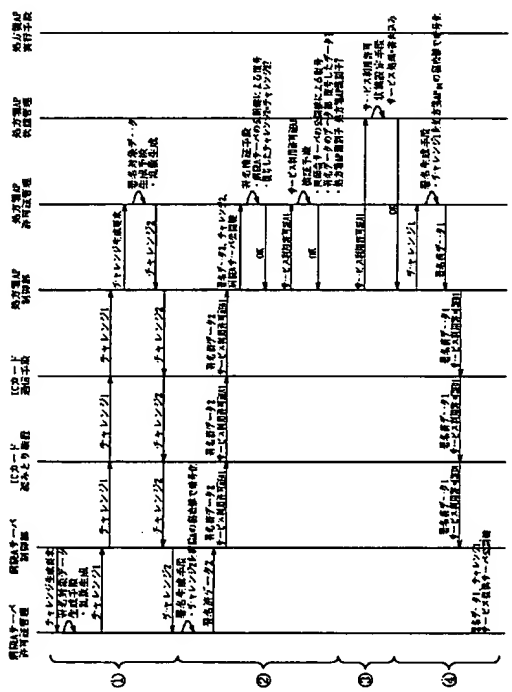
【図８】



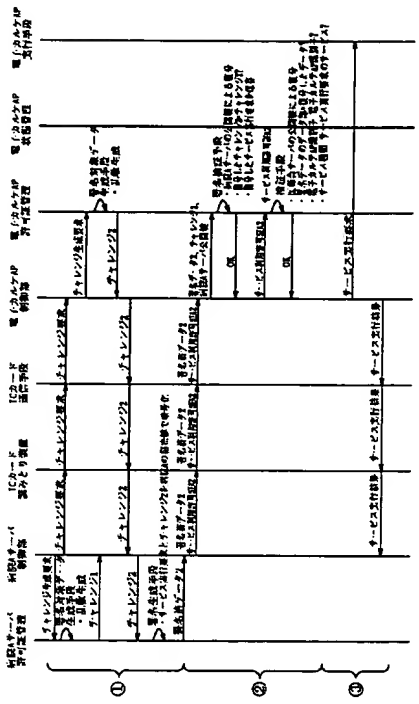
【図９】



【図１０】

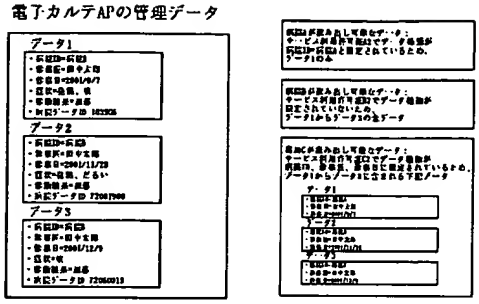


【図１１】



【図１２】

電子カルテAPの管理データ



フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	H04L 9/00 673E	

(72)発明者 南 裕之
大阪府大阪市中央区馬場町３番１５号 西日本電信電話株式会社内

Fターム(参考) 5B058 CA01 KA02 KA04 KA08 KA31 KA35 YA20
5B085 AE09 AE12 AE23 AE29 BE01 BE04 BG01 BG02 BG07
5J104 AA09 LA03 LA05 NA35

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.